American Society of Anesthesiologists®

1501 M Street, N.W. • Suite 300 • Washington, D.C. 20005 • (202) 289-2222 • Fax: (202) 371-0384 • www.asahq.org

Payment and Practice Management Memo
No. 3
October 2013

You Can't Be Too Careful When it Comes to HIPAA Privacy and Security

Since the inception of the Health Insurance Portability and Accountability Act (HIPAA), healthcare organizations have been cautious in the transfer of Protected Health Information (PHI) of patients. PHI refers to individually identifiable health information that is transmitted or maintained by a covered entity and its associations.[1] However, with the substantial amount of information multifaceted healthcare organizations carry today, a potential breach in complying with HIPAA is not as unlikely as you may think.

"Why Is This Relevant?"

Nowadays, HIPAA compliance may be more difficult than it has been in the past. Given recent policies and provisions, all covered entities (which include anesthesia practices) must be more cautious in taking measures to protect both the privacy and the security of the PHI of their patients.

"How Will This Affect *Me*?"

So why is all of this relevant to anesthesiologists? Most medical entities, such as health plans, health care clearinghouses, and health care providers, are familiar with HIPAA, PHI, and the consequences associated with violating patient privacy laws. It may even appear that asking physicians and organizations to brush up on the topic of HIPAA and PHI is trivial. Nevertheless, practices need to be aware that this is more than a nuance. PHI can turn up in unexpected places. In a recent potential violation of HIPAA Privacy and Security Rules, Affinity Health Plan, Inc. will settle with the HHS for $1,215,780 after returning multiple photocopiers to its corresponding leasing companies without obliterating the data contained on the copier hard drives.[2]

FOR IMMEDIATE RELEASE
August 14, 2013

Contact: Office of Civil Rights
(202) 619-0403

HHS settles with health plan in photocopier breach case

Under a settlement with the U.S. Department of Health and Human Services (HHS), Affinity Health Plan, Inc. will settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules for $1,215,780. Affinity Health Plan is a not-for-profit managed care plan serving the New York metropolitan area.

Affinity filed a breach report with the HHS Office for Civil Rights (OCR) on April 15, 2010, as required by the Health Information Technology for Economic and Clinical Health, or HITECH Act. The HITECH Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured protected health information. Affinity indicated that it was informed by a representative of CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity. CBS informed Affinity that the copier that Affinity had used contained confidential medical information on the hard drive.

Affinity estimated that up to 344,579 individuals may have been affected by this breach. OCR's investigation indicated that Affinity impermissibly disclosed the protected health information of these affected individuals when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives. In addition, the investigation revealed that Affinity failed to incorporate the electronic protected health information (ePHI) stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.

"This settlement illustrates an important reminder about equipment designed to retain electronic information: Make sure that all personal information is wiped from hardware before it's recycled, thrown away or sent back to a leasing agent," said OCR Director Leon Rodriguez. "HIPAA covered entities are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals' data, and have appropriate safeguards in place to protect this information."

In addition to the $1,215,780 payment, the settlement includes a corrective action plan requiring Affinity to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent, and to take certain measures to safeguard all ePHI..

HIPAA and PHI violations are more common than not. According to the *24th Annual HIMSS Leadership Survey*, 19% of respondents noted some sort of security breach within their organization in the last year. When asked to identify no more than two concerns they had regarding the security of medical information at their organization, 97% of respondents posed that there was a concern about information security. Top concerning issues in reference to securing information included: Compliance with HIPAA security regulations and CMS security audits and securing information on mobile devices.[3]

"OK, You Have My Attention. So What Should I Expect?"

Meanwhile, The U.S. Department of Health and Human Services (HHS) recently implemented new rules that modify the HIPAA Omnibus Rule, an act enabled to strengthen privacy and security for health information, asking physician practices to update their HIPAA policies and procedures by September 23, 2013, including:

Business Associate Agreements (BAAs) and Notices of Privacy Practices (NPPs). The new rule will also obligate physicians to understand the importance of electronic protected health information.[4]

Correspondingly, on September 16, 2013, the Office of the National Coordinator for Health Information Technology (ONC) and HHS released a model of Notices of Privacy Practices for health care providers and health plans to better regulate communication between patients and plan members. HHS states, *"The HIPAA Privacy Rule gives individuals a fundamental right to be informed of the privacy practices of health plans and health care providers, as well as to be informed of their privacy rights with respect to their personal health information. Health plans and covered health care providers are required to develop and distribute a notice that provides a clear, user friendly explanation of these rights and practices."*[5] Essentially, the new model is in correspondence with the changes regulated by the Omnibus Rule to assist medical entities in upholding privacy requirements**.**

In summary, it can be very easy to violate HIPAA unknowingly through careless handing of private patient information. A vague understanding in the complexity of the laws surrounding HIPAA may play a role in potentially not complying with HIPAA Privacy and Security Rules. To avoid a potential breach, physicians and practices should better their knowledge on such laws and regulations.

For more information on HIPAA's privacy and security requirements, please see:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

Provided on behalf of HHS Office of Civil Rights:

For more information on safeguarding sensitive data stored in the hard drives of digital copiers: http://business.ftc.gov/documents/bus43-copier-data-security

The National Institute of Standards and Technology has issued guidance on media sanitation: http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

OCR offers free training on compliance with the HIPAA Privacy and Security Rules for continuing medical education credit at: http://www.medscape.org/sites/advances/patients-rights

The HHS Resolution Agreement and CAP can be found on the OCR website at:
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/affinity-agreement.html

References:

1. Health Resources and Services Administration. (n.d.). *What is "protected health information" (PHI) and "electronic protected health information" (ePHI) under HIPAA?* Retrieved August 23, 2013, from U.S. Department of Health and Human Services: http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/underhipaa.html

2. Office of Civil Rights. (2013, August 14). *HHS settles with health plan in photocopier breach case.* Retrieved August 16, 2013, from U.S. Department of Health & Human Services: http://www.hhs.gov/news/press/2013pres/08/20130814a.html

3. *HIMSS Leadership Survey.* (2013). Retrieved September 19, 2013, from HIMSS: Transforming Health Through IT: http://himss.files.cms-plus.com/HIMSSorg/Content/files/leadership_FINAL_REPORT_022813.pdf

4. *HIPAA: Health Insurance Portability and Accountability Act.* (n.d.). Retrieved September 16, 2013, from American Medical Association: http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act.page

5. *Health Information Privacy*. (2013). Retrieved September 19, 2013, from U.S. Department of Health & Human Services: http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html